ISSN 1870-4069

A Multilayered Model based on Blockchain that Fortifies the Integrity and Security of Public Information

Fernando Rebollar, Rocío Aldeco-Pérez, Rosa M. Valdovinos, Marco A. Ramos

Universidad Autónoma del Estado de Mexico,
Facultad de Ingeniería,
Mexico

{frebollarc,rvaldovinosr}@uaemex.mx,
marco.corchado@gmail.com,raldeco@unam.mx

Abstract. Digital services have increased proportionately with Internet access. Then, governments in different countries also have increased the digital services they offer to facilitate multiple procedures. As consequence, the use of reliable and transparent systems has become a need. A solution is the use of cryptographic techniques that has culminated in the emergence of blockchain, which allows to decentralize information and build trust and adding smart contracts functionality. However, scalability and speed of transactions are still challenging. Governments from different countries have already evaluated the use of blockchain in their systems, but adaptation strategies and optimization improvements are still required to be successful. This investigation presents a possible solution, adapted to use in government systems, dividing blockchain into multiple organized layers, allowing the use of smart contracts functionality and document storage.

Keywords: Multi-layered blockchain, blockchain, smart contracts, government service.

1 Motivation

As a result of an increased access to Internet, the offer of digital services have grown exponentially [8]. Examples are the governments of developed countries that have increased the number of digital services offered to their citizens and taxpayers [5]. Some of these digital services are created to allow citizens to make payments or to get information about how taxes are invested, spent or allocated. These digital services, even reduce cost and improve efficiency, they lack of transparency on the use of information and consequently decreasing the level of trust in such information that is presented from this government to their citizens.

On these type of digital systems, trust lies on a centralized entity that can be a government employee or an organization depending on the government.

Under this political centralization, digital services become vulnerable, since there is nothing left but to rely on the honesty of these centralized entities. This honesty cannot be enforced neither verified. For this reason, mechanisms that guarantee transparency are necessary so they can facilitate auditing in a decentralized way.

Blockchain has proven to be effective on providing information decentralization [4], while allowing ease of verifying this information transparency, integrity and immutability [10]. Blockchain also makes possible to create the so-called smart contracts [2], which are digital assets containing secure digital agreements that self-execute once the event(s) for which they were designed happen.

The advantages of blockchain have already been recognized by governments of different countries, some of these have already launched projects to incorporate blockchain into digital services, however, they have also found difficult to make it function in the best way [6].

Unfortunately, when blockchain is implemented, a number of challenges that limit its usage are present. For instance, when a considerable number of transactions are created the speed under those transactions are performed and later verified decreases. If smart contracts are added to the picture, then the storage of them became a problem. These challenges are extensively discussed on [9].

A possible solution to the above mentioned challenges is the use of a "multi-layer blockchain". A multi-layer blockchain, as its name indicates, create layers for dividing the different types of information that are stored on such a blockchain. The goal is creating separate blocks that will be accessed only when is required. In that way, performance is improved and information storage can be better manage. [1]

2 Related Work

Cheng and Zhang (2017) in [7] present a proposal for a blockchain-based network model to improve the implementation of IoT devices, maintaining network security by combining cloud storage protocols and proposing two types of layers: external layers and high-level layers. The external layers operate centrally as cloud servers commonly do, while the high-level layers connect to external layers and behave like connected IoT devices. Unlike the outer layer, at the high-level layer, the network is decentralized.

Badr et al. (2018) in [1] describe a multilayer model for clinical patient data, resuming the model proposed by Cheng and Zhang but presenting a configuration in which layers contain 3 main levels. The first level for the patient's devices and sensors, the second level corresponding to hospitals, laboratories, medical bodies, etc. The third tier for centralized cloud storage.

Chang et al. (2018) in [3] propose a two-layer blockchain-based model to preserve clinical patient data while ensuring their privacy. Added deep learning algorithms are used to guarantee data distribution without sacrificing data privacy.

Zhou et al. (2018) in [11] proposes a multilayer architecture from which a cryptocurrency called MOAC is implemented. The proposal maintains security, decentralization and speed of transactions using smart contract functionality through a two-layer splitting. The base layer is used for storing files and the top layer to execute smart contracts.

The majority of the discussed proposals present a two-layer model in which information is separated based on its functionality. However, two layers are not enough because the different types of information contained in the blocks are not separated, which still generates a loss of speed in transactions, this problem gets worse when features like smart contracts are added.

3 Hypothesis

Whit the development of a new multiple layer blockchain were each layer will use a different consensus algorithm, will be possible to guarantee the integrity and security of information while increasing its reliability.

4 Methodology

The proposed methodology considers the following steps:

1. *To study and to analyze the operation of blockchain.* To study and analyze the main cryptographic algorithms used by blockchain, consensus algorithms and mechanisms used to carry out transactions in distributed systems.
2. *To generate the multi-layer model based on blockchain* Once the advantages, disadvantages, compatibilities and incompatibilities of the blockchain types and their consensus algorithms have been identified, a proposal will be built.
3. *To test the previously created proposal and to document the results* Perform a proposal validation through modeling and formalization to validate or refute the hypothesis. The modeling will be carried out using a probabilistic qualitative approach, to infer its behavior.

5 State of the research and Preliminary results

After two years of work, the proposal design is finalized. This proposal presents 4 layers, layer 1: Index-Keys, layer 2: Transactions, layer 3: SmartContracts and layer 4: Files.

By using 4 layers, information can be classified into different types based on the use of each type of information and later be included into the corresponding layer. In this way it is expected to improve the efficiency as transactions will occur in different layers based on functionality.

The next step is to validate the proposal that corresponds to step 3 of the methodology. We believe that given the current state of blockchain a formalization of each layer will help us to verify their behavior. Previous to a formalization is necessary to have a complete model of our proposal. This model will be validated by simulations.

6 Conclusions

Using blockchain-based digital systems can allow transparency and verification of information from government digital systems. It is still necessary to improve the operation of blockchain.

The proposal still needs to be validated and tested so there are no measurable results. However, it is expected that by dividing and organizing the different types of data, a more efficient process that maintain a high rate of transactions will make the use of the blockchain viable in various digital services.

By improving transaction speed and leveraging the functionality of smart contracts, it is possible to streamline, make transparent and automatic various services offered by governments, such as make payments, collections, streamline procedures, etc.

As future work, automatic checks could be added where government digital services are open source. In this way, anyone can download and compare code versions with their cryptographic hash validating that the code that has being released is the same as the one running on the server.

References

1. Badr, S., Gomaa, I., Abd-Elrahman, E.: Multi-tier blockchain framework for iot-ehrs systems. Procedia Computer Science, vol. 141, pp. 159–166 (2018)
2. Buterin, V.: A next-generation smart contract and decentralized application platform. Web: ethereum.org/en/whitepaper/ Accessed 18/09/2020, (2014)
3. Chang, E. Y., Liao, S.-W., Liu, C.-T., Lin, W.-C., Liao, P.-W., Fu, W.-K., Mei, C.-H., Chang, E. J.: Deeplinq: Distributed multi-layer ledgers for privacy-preserving data sharing. In: 2018 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR). pp. 173–178. IEEE (2018)
4. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V., et al.: Blockchain technology: Beyond bitcoin. Applied Innovation, vol. 2, no. 6-10, pp. 71 (2016)
5. Gabison, G.: Policy considerations for the blockchain technology public and private applications. SMU Sci. & Tech. L. Rev., vol. 19, pp. 327–336 (2016)
6. Jun, M.: Blockchain government-a next form of infrastructure for the twenty-first century. Journal of Open Innovation: Technology, Market, and Complexity, vol. 4, no. 1, pp. 7 (2018)
7. Li, C., Zhang, L.-J.: A blockchain based new secure multi-layer network model for internet of things. In: 2017 IEEE International Congress on Internet of Things (ICIOT). pp. 33–41. IEEE (2017)
8. Lipschultz, J.: Free expression in the age of the Internet: Social and legal boundaries. Routledge (2018)

9. Moin, S., Karim, A., Safdar, Z., Safdar, K., Ahmed, E., Imran, M.: Securing iots in distributed blockchain: Analysis, requirements and open issues. Future Generation Computer Systems, vol. 100, pp. 325–343 (2019)
10. Wüst, K., Gervais, A.: Do you need a blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). pp. 45–54. IEEE (2018)
11. Yang, X., DavidChen, X., Zhou, S., Wang, R.: The moac platform: Advancing performance with layered multi-blockchain architecture for enhanced smart contracting. Web: moac.io/uploads/MOAC_White_Paper.pdf Accessed 18/09/2020, (2018)